The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
5/14/2013

SUBJECT:
Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS13-043)

OVERVIEW:
A vulnerability has been discovered in Microsoft Word that could result in remote code execution. Exploitation may occur if a user opens a specially crafted file in an affected version of Microsoft Word or Microsoft Word Viewer. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Office 2003 Service Pack 3
- Microsoft Word Viewer

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A remote code execution vulnerability exists in the way that Microsoft Word processes specially crafted content in Word files. This vulnerability can be exploited if a user opens a specially crafted Word file or previews a specially crafted e-mail with an affected version of Microsoft Word. The specially crafted file can be sent as an email attachment, or hosted on a website.

Successful exploitation of this vulnerability could allow the attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider viewing emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms13-043

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1335